

# Risk Management Framework Glossary

---

Gary E. McGraw, Cigital, Inc. [vita<sup>3</sup>]

Copyright © 2005 Cigital, Inc.

2005-09-21

This glossary contains a list of terms relevant to the Risk Management Framework. The terms defined here are general and are not tied only to the RMF.

## architectural risk assessment

A representation of system risks that exist in the software architecture, including design flaws that directly impact the security of the software. This includes a measurement of impact according to the business situation, an understanding of attacker resources, and likely attack patterns. Sometimes this activity is called *threat modeling* (though this is a misuse of the term *threat* according to the security literature).

## artifact

A product or byproduct of the software development process. Examples include source code, architecture diagrams, requirements documents, a written test plan, results of code reviews, and a report of test results. Analysis of artifacts can provide evidence of a system's quality with respect to various attributes, such as security.

## audit

A review of system security (or software security) in order to provide assurance that the system's security posture is adequate. Comprehensive auditing is a good security practice, but specific kinds of auditing may also be mandated by government, regulatory, or contractual considerations. During software development, this term is often used to refer to a code review or to an architectural risk assessment. In an operational environment, auditing refers to a review of security logs or other data collected during ongoing monitoring of operations to identify actual or attempted security breaches and to evaluate the quality of a system's security. Such auditing should be done frequently, but, unlike intrusion detection approaches, auditing is typically not expected to be a real-time activity.

## bug (implementation)

A software security defect that can be detected locally through static analysis.

## code review

A manual or automated review of computer software, usually source code.

## defect (software)

An implementation or design vulnerability. A defect may lie dormant in software for years and then surface in a fielded system with major consequences.

## FIPS

Federal Information Processing Standard; a set of standards, sometimes related to security, from NIST.

---

3. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/198-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/198-BSI.html) (McGraw, Gary)

## flaw (design)

A software security defect at the architecture or design level. Flaws may not be apparent given only source code of a software system.

## IEC

The International Electrotechnical Commission, founded in 1906. The IEC develops global standards in all areas of electrotechnology. <http://www.iec.ch><sup>4</sup>

## NIST

The National Institute of Standards and Technology, a division of the United States Department of Commerce. NIST issues guidelines and standards for computer security. <http://www.nist.gov><sup>5</sup>

## risk

Flaws and bugs lead to risk. Risks are not failures. Risks capture the probability that a flaw or a bug will impact the purpose of the software. Risk measures also take into account the potential damage that can occur. A very high risk is not only likely to happen but also likely to cause great harm. Risks can be managed by technical and non-technical means.

## risk analysis

*See architectural risk assessment.*

## threat

An actor or agent who exploits security vulnerabilities and risks.

## threat modeling

*See architectural risk assessment.*

## vulnerability

A defect or weakness in system security procedure, design, implementation, or internal control that an attacker can exploit. A vulnerability can exist in one or more of the components making up a system, even if those components aren't necessarily involved with security functionality.

# Cigital, Inc. Copyright

---

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

4. <http://www.iec.ch>

5. <http://www.nist.gov>

1. <mailto:copyright@cigital.com>